



CVE-2021-4076

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-4076
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2022-03-09 19:45:00 UTC
Description	A flaw exists in tang, a network-based cryptographic binding server, which could result in leak of private keys.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tang Project	Tang	All	All	All	All

References

Reference	Source	Link
keys: move signing part out of find_by_thp() and to find_jws() by sergio-correia · Pull Request #81 · latchset/tang · GitHub	MISC	github
2029814 – (CVE-2021-4076) CVE-2021-4076 tang: private key leak	MISC	bugz
keys: move signing part out of find_by_thp() and to find_jws() (#81) · latchset/tang@e82459f · GitHub	MISC	github
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178947](#) Debian Security Update for tang (DSA 5025-1)
- [183579](#) Debian Security Update for tang (CVE-2021-4076)
- [282184](#) Fedora Security Update for tang (FEDORA-2021-aa1d373ed0)
- [282185](#) Fedora Security Update for tang (FEDORA-2021-1fe489496f)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)